1 Technical Management Overview

1.1 Objective

The goal of STS is to partner with the Government of Jordan in helping to ensure and secure a network infrastructure for the E-Government of Jordan Project. The solution should meet the requirements/applications of the Jordan Government and should be accountable to Jordan's overall business strategies and objectives.
The proposed data center solution is around the PIX Firewall and Catalyst 6500 switches; these Cisco's platforms are a key step towards realizing these goals.
Jordan today is evolving their infrastructure to support new business requirements. This includes:

- Web-based services for citizens, connected to the Internet.
- Virtual Private Networks for trusted ministries to access the Data Center via the SGN Network.
- Access for business partners to parts or all of Jordan's E-Government Data Center Network.
- Faster connection for Jordan Online Clients.

The most critical requirement to allow these services is the establishment of a security architecture that protects the resources of E-Government of Jordan, while at the same time allowing users access to the information they require.
This solution proposes Firewall Implementation Services for E-Government of Jordan to enable the PIX Firewall to act as the key security point for connecting the internal Network to the external Internet and to Partners. In addition, the PIX Firewall can act as the key security zone between internal networks that require security services.
The expected benefits include improved authentication, enhanced access control, better information confidentiality and integrity, and improved availability of the network and the attached resources.

1.2 Introduction

The Cisco PIX 535 Firewall is part of the world-leading Cisco PIX Firewall series, providing today's networking customers with unmatched security, reliability, and performance. Ideal for protecting the Data Center's perimeter, the PIX 535 delivers full firewall protection with integrated IP Security (IPsec) virtual private network (VPN) capabilities.

1.3 High Availability

The Cisco PIX Firewall offers unsurpassed reliability, with a mean time between failure (MTB) of more than 60,000 hours. Even with this level of dependability, organizations whose Internet, intranet, or extranet connections are their corporate lifeline know that firewall redundancy is critical. Every minute a firewall is down means lost revenue, opportunity, or critical information.

Cisco has created a failover bundle package for use with the PIX 535, enabling this need to be met simply and inexpensively. This package provides organizations with a second firewall designed to run exclusively in failover mode, for a fraction of the cost of a standard one.

1.4 PIX Architecture overview

STS offered two Front End firewalls for high availability with three Gigabit Ethernet Interfaces and six FastEthernet interfaces.
The interfaces are distributed as following:

- To connect between the two PIX Firewalls for Stateful failover
- To connect to the Internet zone, a Catalyst 2950 has been provided for such purpose
- The Services zone will be connected with Gigabit Ethernet interface
- The Access zone to SGN Network is connected with FastEthernet interface.
- The Email and Content Management zone is connected with Gigabit Ethernet
- The Front End zone is uplinked with gigabit Ethernet interface

The two Back End firewalls are offered with three Gigabit Ethernet Interfaces and six FastEthernet interfaces.
The used interfaces are distributed as following:

- To connect between the two PIX Firewalls for Stateful failover using Fast Ethernet interface
- The management zone will be connected with Fast Ethernet interface
- The Back End Database zone is connected with gigabit Ethernet interface

1.5 Switching Solution

In the Data Center, we will have five Catalyst 6513 Multilayer switches in the core of the network. The Catalyst 6513 is the flagship of Cisco's high level, layer2 to Layer 7-support switch. The Catalyst 6513 will be configured in a fully redundant fashion with Dual Power Supplies and two Supervisor engines and two MSFC-2. The fans and network clocks will also be redundant. The Switching Fabric Module will be included in the chassis to scale the throughput of the backplane from 32Gbps to 256Gbps.

For the server aggregation we will have all the servers connected directly with Gigabit Ethernet to the catalyst 6513 switches. These servers will have dual-homed connectivity to the core switches to increase the availability for the critical servers.

As you can see from the architecture above, we have designed the E-Government of Jordan's network around Cisco's 6513 platforms that will play a key role in network stability and throughput. Cisco's IOS contains a mature set of features that have been carefully refined over many years by Cisco and our customer's real world experience. The Government of Jordan's data center is well served by the Catalyst 6513's and Catalyst 2950 impressive list of features and performance.

The Catalyst 2950 series of switches are proposed for external segment. The Catalyst 2950 series is the highest capacity and most cost effective stickballs in the industry today; they are equipped with a 13.6Gbps fabric and can boost over 7.5 million packets per second in performance. No competitor comes close to matching the flexibility and performance of the Catalyst 2950 series. The Catalyst 2950 does not spare any rich feature either, it fully supports all the requirements for data center, including Security, QoS, Multicast, Resiliency and high performance/bandwidth.

The Catalyst 6500 is Cisco's high end Gigabit Ethernet and Server aggregation switch. It has an unmatched density for up to 130 Gigabit Ethernet ports and supports 32Gbps backplane scalable to 256G. The Catalyst 6500 supports L2-L7 services starting with basic Layer 2 and 3 support, moving to Layer 4 services such as extended Security and QoS, and moving to L4-7 with support for Server Load Balancing and Web Caching/URL filtering. It also supports the PFC (Policy Feature Card), which provides policy networking enforcement at wire speed on all ports.

1.6 E-Government and Web-Scaling

The Cisco Content Switching blade integrated within the Cat6513 enables Government of Jordan engaged in e-business to build global Web networks optimized for e-business transactions and Web content delivery. With its patented content switching technology, the Content switching gives businesses maximum control in ensuring availability of Government of Jordan Web site, securing Web site resources without compromising performance, and allocating Web site resources efficiently.

The content switch is provided to build and scale with the Intranet, extranet and Internet connection for the future. The Content switching blade is suggested in the Services Zone and in the Content Management zone. On those segments, we have a similar design where we are including two Content switching blades connected together back to back or within the same chassis as per the Services zone; running VRRP in between each other with NAT hiding the real IP from outside, these blades are capable of DOS attacks prevention and content awareness.

Benefits of the Content Switching blades:

- Provides high-speed Web content delivery by selecting the best site and server based on full URL, cookie, and resource availability information
- Offers site-level security with wire-speed denial-of-service (DoS) prevention; firewall load-balancing provides scalable security for web servers
- Delivers up to 400 percent improvement in Web cache efficiency for transparent, proxy, and reverse proxy configurations
- Supports all TCP- and UDP-based Web protocols, wire-speed network address translation (NAT), and integrated IP routing
- Optimizes both content requests and delivery for HTTP, passive File Transfer Protocol (FTP), and streaming media protocols
- Enables advanced service level agreements (SLAs), and a variety of new fee-based services

Featuring patented content-switching technology, Cisco Content switching blade gives Government of Jordan businesses maximum control in allocating e-business site resources and building services for optimal return on investment (ROI). By implementing Content Switching Network Services for e-business, Government of Jordan their hosting partners/Ministries can provide reliable, secure, high-performance e-government sites that are continuously "open for business."

1.7 Internal Network Security

According to FBI, 80% of the attacks are from the internal users; hence, STS's consultant suggests using an intrusion detection system IDS.
We included in our Solution two IDS. One located on the external segment and one located on the SGN segment These IDS have the following features listed below.

Sophisticated Attack Detection and Antihacking Protection:

- *Exploits*—Activity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
- *Denial-of-service (DoS)*—Activity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
- *Reconnaissance*—Activity indicative of someone probing or mapping your network to identify "targets of opportunity," such as ping sweeps and port sweeps; usually a precursor to an actual exploit attempt
- *Misuse*—Activity indicative of someone attempting to violate corporate policy; this can be detected by configuring the sensor to look for a custom text strings in the network traffic; for example, XYZ Corporation could easily configure the Cisco Secure IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP)
- Real-time capability, as opposed to a periodic review of log files, can significantly reduce potential attack damage and recovery costs by eliminating a hacker from the network
- By presenting decision-critical intrusion alarm information, such as offending and destination IP addresses, destination port, and attack descriptions, users can develop metrics and track trends to determine the security state of a network
- Information can be ported to a relational database and provide the basis for more accurate, fact-based decision-making regarding the security of the network

1.8 Management Solution

As part of phase 1, we are providing CiscoSecure Access Control Server, which includes Radius and TACACS+. This Authentication, Authorization and Accounting software will help E-Government of Jordan to authenticate against any connection from inside to outside or outside to inside and it is highly advisable to be used with the VPN concentrators and for VPN Clients. Unlimited number of VPN Clients license will be delivered part of this solution with zero Dollar value.

The CiscoSecure VPN/Managed Services will include CiscoSecure Policy Manager, which will help firewall administrators to manage and enforce policies on the PIX Firewall through a GUI Interface eliminating the need to handle the IOS commands. As

well, the CSPM is used to manage the Intrusion Detection System's Signatures and attacks Database monitoring.

1.9 Design Summary

As you can see from the architecture above, we have designed E-Government of Jordan's network around Cisco's platforms that will play a key role in network stability and throughput. Cisco's IOS contains a mature set of features that have been carefully refined over many years by Cisco real world experience. E-Government of Jordan's network is well served by Cisco Product impressive list of features and performance and STS Professional skills build over years.